# North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

## NDSLIC Disclaimer



## Quick Links

## North Dakota

**Hackers target small businesses.** The Better Business Bureau of Minnesota and North Dakota, and the Minnesota Cyber Crime Task Force are urging all small businesses with outdated or lacking online security software to be aware of foreign hackers stealing credit card information and then selling it on the Web. Businesses targeted by these cyber intrusions could be liable for any losses involving stolen credit card data, which could potentially bankrupt smaller enterprises. All small businesses that process, store or transmit credit card information are advised to bring up to date their security software and become PCI compliant immediately. The Payment Card Industry Data Security Standard is a set of requirements designed to ensure that all companies that deal with credit card information maintain a secure environment. Although the PCI is not law, it was created by major credit card brands that can, at their discretion, fine merchants that do not comply with the standards in case of a data breach. Source: http://www.thenewnewinternet.com/2010/05/26/hackers-target-small-businesses/

## Regional

(Minnesota) **E. coli outbreak in Minnesota tied to raw milk.** A Minnesota toddler has been hospitalized with a life-threatening illness and three other people have been sickened by E. coli-tainted raw milk, an outbreak that is likely to sharpen a national debate on the growing popularity of the controversial beverage. Three of the four E. coli 0157:H7 cases are linked to unpasteurized milk produced at the Hartmann Dairy Farm in Gibbon, Minnesota, which is also known as M.O.M.s, or Minnesota Organic Milk, state health and agricultural department officials said May 26. They said consumers should discard any dairy products — including cheese and ice cream — made by Hartmann. None of the milk involved so far appears to have been sold in stores, said the Minnesota Department of Agriculture's director of dairy and food inspection. Raw milk hasn't been pasteurized — that is, treated with heat to kill organisms that can make people sick. Interstate sales of raw milk are banned, but more than 20 states allow sales — usually limited — of the product. In Minnesota, raw milk is restricted to "occasional purchases directly at the farm where the milk is produced," the dairy and food inspection director said. Source: http://www.startribune.com/lifestyle/health/94980484.html?elr=KArksLckD8EQDUoaEyqyP4O:DW3ckUiD3aPc:_Yyc:aUnciaec8O7EyUsl

(Minnesota) **Automatic shutdown of Prairie Island nuclear power plant under investigation.** Prairie Island operators are trying to figure out what tripped a turbine at the nuclear power plant in Red Wing, Minnesota, automatically shutting down one of its two units Tuesday. The plant's owner, Xcel Energy, said there were no injuries, no release of radiation and no threat to the public. The reactor was being returned to full power Monday after it was shut down for refueling and maintenance April 17. Operators said it was about 32 percent of power capacity when the turbine tripped about 3 a.m. Tuesday. The plant's other reactor was not affected and continues to operate at 100 percent power. Xcel Energy said each unit generates about 550 megawatts of power, which together, provides

enough energy to power nearly 1 million homes. Source: http://www.wctrib.com/event/article/id/67907/group/homepage/

(Minnesota) **1 bank closed on May 21. State and federal regulators closed one bank May 21.** This closing raises to 81 the number of failed institutions so far in 2010. Pinehurst Bank in St. Paul, Minnesota was closed by the Minnesota Department of Commerce, which appointed the Federal Deposit Insurance Corporation as receiver. Coulee Bank, La Crosse, Wisconsin, will buy all of the deposits of Pinehurst Bank. The sole branch of Pinehurst Bank will reopen as a branch of Coulee Bank. Pinehurst Bank had approximately $61.2 million in total assets. The estimated cost to the Deposit Insurance Fund (DIF) will be $6 million Source: http://www.bankinfosecurity.com/articles.php?art_id=2566

(South Dakota) **Bank alerts members to phishing scam.** Sentinel Federal Credit Union is alerting the Rapid City, South Dakota community of a telephone scam that has targeted the area over the past several days. This scam, called phishing, attempts to steal personal information. In the scam, people are receiving fraudulent automated messages stating their Sentinel Federal Credit Union ATM or debit card has been compromised. The automated message then instructs the caller to enter their card number to reactivate the card. Sentinel Federal Credit Union said it will never contact its members this way. Source: http://www.rapidcityjournal.com/news/article_9aa5f490-6783-11df-ab19-001cc4c03286.html

## National

**Pirates terrorize boaters on Texas lake along Mexican border.** With machine guns in hand, Mexico's deadliest cartel is patrolling Mexican territory in the waters of a Texas border lake. The pirates already have hit several boats on Falcon Lake near Zapata, which is about an hour south of Laredo. At least three boats have been robbed so far, and authorities say they are investigating a possible fourth incident. The fear of what lurks beyond the boundary is keeping even local fisherman well within the U.S. side of the lake. U.S. authorities said there just is not a Mexican law presence on the other side of the lake, so boaters who do venture to that part of Falcon Lake are on their own. Source: http://www.kens5.com/news/pirates-94535754.html

## International

**Suspected sabotage derails train in India; 71 dead.** Suspected Maoist rebels derailed an overnight passenger train Friday in eastern India, triggering a crash with an oncoming cargo train that killed at least 71 people and injured about 200 more, officials said. Survivors described a night of screaming and chaos after the derailment, and said it took rescuers more than three hours to reach the scene. The blue passenger train and the red cargo train were knotted together in mangled metal along a rural stretch of track near the small town of Sardiha, about 90 miles west of Calcutta in West Bengal state. Officials disagreed on the cause of the derailment, with some saying it was caused by an explosion but others blaming sabotaged rail lines. The Indian Home Minister said in a statement that a section of the railway tracks had been cut, but "whether explosives were used is not yet clear." The top police official in West Bengal said posters from the People's Committee Against Police Atrocities, a group local officials believe is closely tied to the Maoists, had been found at the scene taking responsibility for the attack. However, a spokesman for the group denied any role, the Press Trust of

India news agency reported. “We were in no way involved. This is not our act,” PTI quoted him as saying by phone. Source: http://www.ajc.com/news/nation-world/suspected-sabotage-derails-train-536993.html

**Death toll from south Russia bomb rises to seven.** The death toll from a bomb blast in the southern Russian city of Stavropol rose to seven May 27, and 16 people are in a critical condition. The bomb, equivalent to 400 grams of TNT, was disguised as a pack of juice. The blast occurred May 26 just before the start of a concert by a dance company linked with Kremlin-backed Chechen President Ramzan Kadyrov. Russia said investigators had opened a criminal case under terrorism laws after the blast in the ethnically Russian Stavropol region, which borders the violence-racked, mainly Muslim republics of the North Caucasus. A Stavropol doctor told Rossiya-24 television that the death toll had risen by two overnight to seven, and that 16 people were in an “extremely grave condition” with chest, abdominal, and head wounds. Source: http://www.reuters.com/article/idUSTRE64P48I20100527

**Romanian authorities shut down ATM-skimmer manufacturing operation.** The Romanian organized crime police has dismantled a major cybercriminal ring that specialized in manufacturing and selling ATM skimmers. Law enforcement officials descended at more than 40 locations in several cities and detained 20 suspects. Prosecutors from the Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) are investigating multiple individuals under the suspicion of being members of an organized crime group, unauthorized access to a computer system, possessing card-cloning equipment, access-device fraud, and distributing fake electronic-payment devices. According to DIICOT, the criminal group operated out of Romania’s Dolj county, particularly the city of Craiova, where the ATM skimmers were assembled. However, some of the electronic components used for the devices were manufactured in Bucharest. The devices were either sold to other fraudsters or used by ring members in Italy, Germany, Sweden, or Romania. Teams of Romanian Police special forces raided 38 locations in Craiova, six in Bucharest and three in a neighboring county earlier today, taking a total number of 20 suspects back for questioning. Amongst them are the brother of a local magistrate and the son of a Ministry of Interior official. Source: http://news.softpedia.com/news/Romanian-Authorities-Shut-Down-ATM-Skimmer-Manufacturing-Operation-143204.shtml

**60 arrested over Kachin dam bombs.** A major police operation in Burma’s northernmost Kachin state netted around 60 people last night suspected to have been involved in the bombing of the Myitsone dam in April. A resident of Myitkyina, capital of Kachin state told DVB that the operation involved police, ward officials, anti-narcotics agents, as well as the tactical operations commander of the Burmese army’s Northern Command. At least three bombs exploded at the controversial Myitsone dam site, killing three and injuring 20. The explosions occurred in the compounds of the Asia World Co. Ltd, which is building the dam and all three victims were company employees. The compound is located 18 miles north of Myitkyina. Posters were placed around Myitkyina displaying sketches of the suspects and announcing rewards for their capture. On the night of May 26 alone, about 60 people were taken into custody from [Kya Zu] ward. Some of the detainees were freed later. Source: http://www.dvb.no/news/60-arrested-over-kachin-dam-bombs/9176

**German bank ‘blown up by robbers.** Suspected robbers in Germany appear to have miscalculated the quantity of explosives needed to blow their way into a rural bank. The building housing the bank

in the northern village of Malliss was largely destroyed by an overnight explosion. The bank's cash machine survived intact and the suspected thieves are not thought to have made away with any money, Germany's Welt Online reported. No one was injured, though the blast damaged nearby cars and buildings. Investigators were working on the assumption that robbers had placed their explosives, possibly made from petrol or acetylene, at the entrance to the bank, German broadcaster NDR said. The presence of a delivery van near the site of the explosion indicated that the suspected thieves may have intended to drive off with the cash dispenser, local media reported. Source: http://news.bbc.co.uk/2/hi/world/europe/10161486.stm

**Dozens killed in Jamaican violence.** The United States shut its embassy in Jamaica, Tuesday, with only essential staff reporting to work, as violence continues to escalate in the island nation's capital of Kingston. The embassy also suspended all visa operations and nonessential services for Americans, a State Department spokesman said. A travel alert remains in effect for the area. The State Department issued the alert Friday after masked men defending a reputed drug kingpin who the U.S. has been trying to extradite since August, went rampaging through the streets of Kingston. Twenty-seven people have been killed and 31 wounded in an assault on the suspected drug lord's compound, Jamaican police said Tuesday. The problems began over the weekend when the kingpin's supporters barricaded themselves behind a makeshift fortress of junk cars and barbed wire. The Jamaican government declared a state of emergency as the situation intensified. Source: http://edition.cnn.com/2010/WORLD/americas/05/25/jamaica/index.html

**Pakistan arrests many over Times Square bomb plot.** Pakistan has arrested several suspects in connection with the failed bombing in New York City. Pakistani officials told news agencies one of the arrested is the co-owner of a prominent catering firm used by the U.S. embassy in Islamabad. It is not clear when the arrests were made. They follow a visit to Pakistan by two senior U.S. security officials. Source: http://news.bbc.co.uk/2/hi/world/south_asia/10140288.stm

## Banking and Finance Industry

**Cyber thieves rob Treasury Credit Union.** Organized cyber thieves stole more than $100,000 from a small credit union in Salt Lake City last week, in a brazen online robbery that involved dozens of co-conspirators, KrebsOnSecurity has learned. In most of the e-banking robberies written about to date, the victims have been small to mid-sized businesses that had their online bank accounts cleaned out after cyber thieves compromised the organization's computers. This incident is notable because the entity that was both compromised and robbed was a bank. The attack began May 20 when the unidentified perpetrators started transferring funds out of an internal account at Treasury Credit Union, a financial institution that primarily serves employees of the U.S. Treasury Department and their families in the state of Utah. The Treasury Credit Union president said the thieves made at least 70 transfers before the fraud was stopped. Many of the transfers were in the sub-$5,000 range and went to so-called "money mules," willing or unwitting individuals recruited over the Internet through work-at-home job schemes. The credit union president said other, larger, transfers appear to have been sent to commercial bank accounts tied to various small businesses. According to the credit union president, the perpetrators who set up the bogus transactions had previously stolen a bank employee's online log-in credentials after infecting the employee's Microsoft Windows computer with a Trojan horse program. He said investigators have not yet determined which particular strain of malware had infected the PC, adding that the bank's installation of Symantec's Norton Antivirus failed

to detect the infection prior to the unauthorized transfers. Source: http://krebsonsecurity.com/2010/05/cyber-thieves-rob-treasury-credit-union/

**Cyber thieves rob Treasury Credit Union.** Organized cyber thieves stole more than $100,000 from a small credit union in Salt Lake City last week, in a brazen online robbery that involved dozens of co-conspirators, KrebsOnSecurity has learned. In most of the e-banking robberies written about to date, the victims have been small to mid-sized businesses that had their online bank accounts cleaned out after cyber thieves compromised the organization's computers. This incident is notable because the entity that was both compromised and robbed was a bank. The attack began May 20 when the unidentified perpetrators started transferring funds out of an internal account at Treasury Credit Union, a financial institution that primarily serves employees of the U.S. Treasury Department and their families in the state of Utah. The Treasury Credit Union president said the thieves made at least 70 transfers before the fraud was stopped. Many of the transfers were in the sub-$5,000 range and went to so-called "money mules," willing or unwitting individuals recruited over the Internet through work-at-home job schemes. The credit union president said other, larger, transfers appear to have been sent to commercial bank accounts tied to various small businesses. According to the credit union president, the perpetrators who set up the bogus transactions had previously stolen a bank employee's online log-in credentials after infecting the employee's Microsoft Windows computer with a Trojan horse program. He said investigators have not yet determined which particular strain of malware had infected the PC, adding that the bank's installation of Symantec's Norton Antivirus failed to detect the infection prior to the unauthorized transfers. Source: http://krebsonsecurity.com/2010/05/cyber-thieves-rob-treasury-credit-union/

**Phishing scam targets military credit unions.** U.S. Strategic Command officials are joining leading security software vendors in warning soldiers serving in the U.S. Armed Forces to be on high alert for a new phishing scam that targets customers at a pair of credit unions catering to servicemen and their families. The STRATCOM commander is warning soldiers and their families that bogus Web sites imitating both USAA, a popular insurance and financial services firm catering to military families, and the Navy Federal Credit Union have successfully stolen the personal and banking data of an unknown number of customers. In a blog posting this week, Symantec officials said the phishing sites ask customers to fill in a form with their sensitive data to unlock what the corrupt Web page claims is a login error created by too many failed login attempts. This information includes social security numbers, credit card information, birth dates and mothers' maiden names. "The page also includes a fake CAPTCHA that accepts data irrespective of the number entered," Symantec's security team wrote. "When the sensitive information is entered, the phishing site states that the customer's password is unlocked for logging in. The page is then redirected to the legitimate site." Source: http://www.esecurityplanet.com/news/article.php/3884866/Phishing-Scam-Targets-Military-Credit-Unions.htm

**Gas stations protect customers from 'skimming'.** Criminals have found an easy way to make money — breaking into gas pumps and installing tiny card-skimming machines that can read credit cards. It has become such a worldwide problem, that as of this summer, credit card companies are requiring all gas station owners to purchase and install new technology to curtail the crime. "The penalties are stiff," said a West Palm Beach, Florida Exxon owner. "If we do not upgrade, we will not get to take credit cards and that's 90 percent of our business." The cost is roughly $4,000 per pump. Add that to requirements for station generators and hurricane-proof pumps, and the Exxon owner fears the few

little guys in the gas station business may be driven out of business. All stations are required to have the new technology by June 30. There is one exception, because of an equipment shortage, Exxon and Mobil stores, have been given an extension until December. Source: http://www.wptv.com/content/news/centralpbc/westpalmbeach/story/Gas-stations-protect-customers-from-skimming/4pMYf6EWvEuMkPrXD_F0nw.cspx

**Fidelity Bank issues warning about fake cashier's checks.** The Fidelity Bank, which has 15 branches in the Triad, said May 24 that it has notified the Federal Deposit Insurance Corp. that counterfeit cashier's checks bearing its name are in circulation. The counterfeit items display the routing number 053103585, which is assigned to the bank. The items are markedly dissimilar to authentic checks. The words "cashier's check" are shown inside of a box in the top-center area. A security feature statement appears below the border on both sides of the box. A security feature statement also appears across the bottom of the items. The phrase "authorized signature" is shown below the signature line in the lower-right corner. According to the bank, authentic cashier's checks are gray. The words "cashier's check" are in the top-center area with horizontal lines on both sides. A "notice to customers" statement appears inside of a box below the written amount line on the left side of the checks. Source: http://www2.journalnow.com/content/2010/may/25/fidelity-bank-issues-warning-about-fake-cashiers-c/news-regional/

**Walmart to support smartcard payments.** Retail giant Walmart Stores Inc. is reportedly planning on making all its payment terminals in the U.S. compliant with a smartcard-based credit card technology that is widely used around the world but is not common in the U.S. Walmart's plans were disclosed at a smartcard conference being held this week, and were first reported by Storefront Backtalk. Storefront Backtalk quoted Walmart's director of payment services as saying the retailer was working on making all payment terminals in its domestic stores chip-and-PIN-capable. The director was reported as having said that signature-based credit-card transactions had become a "waste of time" for Walmart. Such a move by Walmart would have widespread ripple effects. As the largest retailer in the world, a Walmart decision to support chip-and-PIN could finally nudge card issuers, payment processors and other merchants to adopt the technology. Source: http://www.computerworld.com/s/article/9177056/Wal_Mart_to_support_smartcard_payments

(Colorado) **Phone scam asking for credit card number targets region.** A phone scam is making its way throughout the region, asking customers for their credit card numbers in order to protect against future fraud. The scam works by trying to make an individual think they are already a victim of fraud. The caller tells the potential victim that someone has made fraudulent charges on the victim's card, and in order to stop it, they need the credit card number. Aventa, which was formerly Colorado Springs Credit Union, is sometimes referenced in these scam calls, and a company representative said it has already started receiving calls from concerned customers. Aventa's representative said customers should never give out personal and account information; if one's financial institution needs it, they probably already have it. Source: http://www.kktv.com/news/headlines/94711734.html?ref=734

## CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

## COMMERCIAL FACILITIES

(Ohio) **Suspicious device destroyed by bomb squad.** Dublin, Ohio police, the Columbus Bomb Squad, and the state arson squad are investigating a suspicious device that was destroyed May 26 at a Dublin residence. Police and Washington Township Fire Department firefighters were called to the scene around 10:38 a.m. by residents of the property where the device was found. The device was examined and eventually rendered safe by the bomb squad. Police said the resident was notified he could return home after the device was rendered safe, but he chose to go to a hotel for the evening. The materials the device was constructed of have been collected for testing. At this time, no charges have been filed, and the incident remains under investigation. Source: http://www.columbuslocalnews.com/articles/2010/05/26/dublin_news/news/police_beat/dudevice5_20100524_0912pm_4.txt

(Arizona) **Suspected bomb in bag closes Fry's parking lot in Avondale.** Avondale, Arizona police closed off a Fry's grocery store parking lot and gas station May 24 after two transients found a suspected explosive device inside a bag. The woman and a man, both transients, had found the bag in a dumpster behind an apartment complex near 103rd Avenue and Camelback Road in west Phoenix. They opened the bag for the first time outside the Fry's store and called police after finding several, small gray cylinder items taped together with possible wires attached. Officers determined the materials looked like a bomb and called in the Maricopa County Sheriff's Office bomb squad. Deputies took the device off site and destroyed it. No one was injured. Source: http://www.azcentral.com/community/swvalley/articles/2010/05/26/20100526phoenix-bomb-scare-avondale.html

(Florida) **Mall evacuated, suspicious package found.** A Kissimmee, Florida mall was evacuated after a suspicious package was found May 22. The package turned out to be a suitcase wrapped in duct tape with a Mexico sticker on it. Kissimmee police evacuated the east side of Osceola Square Mall after someone found the suitcase in the parking lot. They later determined the suitcase was not dangerous. It has not been determined who the suitcase belonged to. Source: http://www.cfnews13.com/News/Local/2010/5/22/mall_evacuated_suspicious_package_found.html?refresh=1

(Texas) **Bomb squad blows up 'suspicious' device at North Side building.** A team from the San Antonio Police Department Bomb Squad blew up a suspicious package at a North Side building, Monday afternoon. The San Antonio Fire Department and San Antonio Police Department were called to a building in the 300 block of East Nakoma after the package was found inside a ladies restroom. A police department spokesperson said the building was evacuated, officers blocked off an area around the building, and the package was blown up. Officials said the "homemade" device was a hoax and turned out to be 3 PVC pipes in a pink container that did not contain anything dangerous. No injuries were reported. Source: http://www.woai.com/news/local/story/Bomb-squad-blows-up-suspicious-device-at-North/U3tk5aPRkEyPmc-HmDVcOw.cspx

(West Virginia) **One dead after explosive device detonated outside club.** A person detonated an explosive device outside of a Huntington, West Virginia nightclub early May 22, killing himself; but he clearly had the intentions of killing others. The co-owner of the nightclub said that the 45-year-old man responsible was banned from her bar, because he came there to stalk his ex-wife. The explosion,

which happened around 3 a.m., shut down Route 60, and put the lives of dozens of families at risk. Homes in the area of the bar were also evacuated. The man was at the nightclub wearing a disguise and had a bomb in his pocket. Investigators said the death toll could have been much higher. They discovered several more live suspicious devices outside the bar. The name of the man has not been released. Source: http://www.wsaz.com/news/headlines/94645894.html?ref=894

(California) **Bomb squad explodes grenade found in downtown Napa.** Law enforcement officials detonated what they believed was an explosive device found in bushes near Exertec Fitness Center in downtown Napa May 19. No one was hurt in the blast. At about 11 a.m., city workers trimming the bushes in a planter that lines the fitness center's Clay Street parking lot spotted what appeared to be an old military-style grenade. Police told people to stay in the fitness center and several other surrounding buildings. A few buildings were evacuated, and officials closed sections of Seminary, Clay and Franklin streets and other nearby roads for about three hours. A deputy from the Napa County Sheriff Office's Bomb Squad put on an 80-pound protective suit and entered the area where officials had set up sand bags in the middle of Clay Street. The deputy attempted to X-ray the suspected grenade, but he was unable to do so because of its position. Instead, he attached a rope to the device, then stood back and dragged it across the street into the sandbags. He then packed other explosives and sandbags around the device and left the area. From about a block away, other officers detonated the grenade at 12:47 p.m. The explosion blew sand 25 to 30 feet in the air. People were released from where they were advised to stay in at about 1:10 p.m., and all streets were open again at about 2 p.m. Source: http://www.sthelenastar.com/articles/2010/05/22/news/saturday_update/doc4bf6c22439f84494594436.txt

## Communications Sector

**AT&T digital network outage silences landlines.** AT&T's new digital home phone service failed across the country Tuesday, illustrating continuing reliability issues with Internet-based phone service. Customers of AT&T Inc.'s U-Verse Voice said their landline phones have had no dialtones since the morning. Reached by cell phone, the customers said those who call them get a message that the line has been disconnected. Support personnel are telling customers that a server crash brought down U-Verse Voice in AT&T's entire 22-state local-phone service area. AT&T spokeswoman said the outage started at about 10:30 a.m., and service was restored to most subscribers at 2:45 p.m. She said the extent of the outage was unknown. Source: http://www.cbsnews.com/stories/2010/05/26/tech/main6519669.shtml

**US begins $8 billion upgrade of GPS satellites.** The U.S. is upgrading its 24 Global Positioning System (GPS) satellites in a bid to improve the accuracy of the technology and prevent outages. As part of the $8 billion upgrade, 18 new satellites are being built by Boeing's Space and Intelligence Systems, while Lockheed Martin has been commissioned to build a further 12 satellites. Each of the existing 24 satellites will be replaced, the first of which was launched this weekend, while the remaining six that have been manufactured will be kept as spares. "We know that the world relies on GPS," the upgrade's chief engineer told the Los Angeles Times. It is thought the new satellites will mean a location can be pinpointed to "within an arm's length, compared with a margin of error of 20 feet or more today." The upgrade is expected to take 10 years to complete and will be handled by engineers

at the Los Angeles Air Force Base in El Segundo. Source: http://www.networkworld.com/news/2010/052410-us-begins-8bn-upgrade-of.html

## DEFENSE INDUSTRIAL BASE SECTOR

(Florida) **Boeing receives 1st F-16 for conversion into QF-16 aerial drone.** The first retired F-16 Falcon arrived at Boeing's Cecil Field facility in Jacksonville, Florida April 22 to begin conversion into a QF-16 aerial drone. Boeing received a $69.7-million contract from the U.S. Air Force March 8 for the first phase of the QF-16 program. The Boeing-led team will begin engineering, manufacturing and development of the full-scale manned and unmanned QF-16s during Phase 1. The drones will be used as aerial targets for newly developed weapons and tactics. They will be a higher-performing aircraft than the QF-4s they will replace. The team will receive six F-16s during the program's development phase. After modification to the QF-16 configuration, they will serve as prototypes for engineering tests and evaluation prior to low-rate initial production. Up to 126 QF-16 drones will be converted beginning in 2014. Source: http://boeing.mediaroom.com/index.php?s=43&item=1229

**New Lynx AMR successfully integrated and flown on a Predator B UAS.** General Atomics Aeronautical Systems, Inc., a leading manufacturer of Unmanned Aircraft Systems (UAS), tactical reconnaissance radars, and surveillance systems, May 27 announced that it has successfully completed a set of flight tests of its next generation Synthetic Aperture Radar/Ground Moving Target Indicator (SAR/GMTI) radar, the Lynx Advanced Multi-channel Radar (AMR), on the company's capital Predator B UAS. The flights were completed May 7 at GA-ASI's Gray Butte Flight Operations Facility in Palmdale, Calif., following software testing and aircraft payload integration. "This first flight of the Lynx AMR on Predator B marks the first time that radar dismount detection capability has been demonstrated on a Predator-class aircraft," said the president of Reconnaissance Systems Group, General Atomics Aeronautical Systems, Inc. Source: http://nosint.blogspot.com/2010/05/new-lynx-amr-successfully-integrated.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

**US Air Force tests hypersonic cruise missile.** The U.S. Air Force Wednesday test launched a hypersonic cruise missile, with the vehicle accelerating to Mach 6 before splashing down in the Pacific Ocean, officials said. The Air Force said the test flight of the X-15A Waverider lasted more than 200 seconds, the longest ever hypersonic flight powered by scramjet propulsion. The previous record was 12 seconds in a NASA X-43 vehicle. "We are ecstatic to have accomplished most of our test points on the X-51A's very first hypersonic mission," said the program manager with the Air Force Research Laboratory at Wright-Patterson Air Force Base in Ohio. Source: http://nosint.blogspot.com/2010/05/us-air-force-tests-hypersonic-cruise.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence)

**Aerojet validates engine design for Orion crew exploration vehicle.** Aerojet has completed a second set of hot-fire test sequences of its R-1E 25-pound thrust, bipropellant engine. This second test included more than 17,250 seconds of total burn time, demonstrating engine flexibility to operate under a broad variety of conditions expected for NASA's Orion service module. Initial test results indicate the engine performed successfully in simulated space-flight mission scenarios. Lockheed

Martin is NASA's prime contractor for developing the Orion crew exploration vehicle as the nation's next generation spacecraft for future exploration throughout the solar system. Aerojet is providing all of the engines for the Orion spacecraft, which is comprised of a crew module for crew and cargo transport, and a service module for propulsion, electrical power and fluids storage. Risk reduction testing of critical subsystems has been ongoing throughout Orion's development phase to maximize mission success and crew safety. This early demonstration of the engine's performance at expected Orion operating conditions was conducted to retire risk to the Orion vehicle including sustained operation at severe conditions. Source: http://www.space-

## Critical Manufacturing

**2010 Nissan, Infiniti trucks, SUVs recalled.** Nissan North America is recalling several 2010 Nissan and Infiniti trucks and SUVs to fix a problem with the front suspension. The company said some lower control link assemblies might not be properly welded. If the weld separates, vehicle handling could be affected, possibly causing a crash. The affected models and model years are: 2010 QX56, 2010 Armada, 2010 Frontier, 2010 Pathfinder, 2010 Titan, and 2010 Xterra. The affected vehicles were manufactured from November 19, 2009 through March 3, 2010. Dealers will repair the vehicles free of charge when the recall begins in June. Source: http://www.consumeraffairs.com/recalls04/2010/nissan_trucks.html

**Lexus models recalled to fix steering problem.** Toyota is recalling about 3,800 Lexus models to fix a problem with the steering system. The company said the steering wheel could become off-center by as much as 90 degrees after a sharp turn, possibly causing a crash. Models and model years affected by the recall are: Lexus 2009-2010 LS460 and LS460L, 2010 LS600H, and LS600HL. Dealers will replace the steering control unit free of charge. Source: http://www.consumeraffairs.com/recalls04/2010/lexus_steering.html

**2010 Ford Ranger pickups recalled.** Ford is recalling about 2,900 2010 Ranger pickups equipped with manual transmissions because of a problem with the parking brake. The company said the brake cable could become disconnected from the right rear actuator during cold weather, causing excessive pedal travel when the brake is applied. If the brake is not fully applied, the vehicle could roll away. The recalled vehicles were manufactured from June 8, 2009 through February 2, 2010. Dealers will install a revised brake actuator when the recall begins this month. Source: http://www.consumeraffairs.com/recalls04/2010/ford_ranger.html

**House bill mandates 'black boxes' for all cars.** On a 31-21 vote, the House Energy and Commerce Committee has approved a bill that, among other things, would require all vehicles sold in the U.S. to be equipped with a "black box" that records crash data by 2015. The Motor Vehicle Safety Act now goes to the full House for debate. The Senate is considering a similar measure. Included in the bill is a requirement for automakers to provide an emergency brake override system that could stop the car if the throttle were stuck in the open position. That provision was added in the wake of Toyota's well-publicized unintended acceleration problems that forced a large recall earlier this year. The measure also includes a provision increasing the maximum penalty on carmakers that fail to report defects. Toyota has paid a record $16.2 million fine in connection with its unintended acceleration problems. Some tougher provisions of the bill were removed after objections from the auto industry. However, the Alliance of Automobile Manufacturers said it is generally in favor of most of the bill's provisions,

including the emergency brake override system and the inclusion of a "black box" data recorder. The measure would give new power to the National Highway Traffic Safety Administration (NHTSA). The agency would be authorized to order recalls that "present a substantial likelihood of death or injury to the public." To increase NHTSA's budget, the measure would add a $9 tax per car — ultimately to be paid by the purchaser — with the money going directly to fund the agency's operations. Source: http://www.consumeraffairs.com/news04/2010/05/autos_black_box.html

**Toyota sudden acceleration may be tied to 89 deaths.** Toyota vehicles in unintended acceleration crashes may be linked to 89 deaths since 2000, up from 52 reported in March, the U.S. National Highway Traffic Safety Administration (NHTSA) said. The deaths occurred in 71 crashes allegedly caused by the vehicle defect, more than the 43 reported in March, the agency said today, citing data through May 20, in an e-mailed response to a request for the data. The agency has received 6,200 complaints where drivers reported sudden, unintended acceleration in Toyota vehicles from 2000 to mid-May, the agency said, up from 2,600 reported in March. The cases in NHTSA's database are submitted by the public and not every incident may be verified. Regulators have not found evidence to warrant a new defect investigation after speaking to 100 car owners who complained about sudden acceleration following repairs Toyota made to their vehicles, the NHTSA administrator said at a May 20 House hearing. Toyota, the world's largest automaker, hasn't found any electronics flaws after examining more than 2,000 vehicles that would help explain the reports of sudden acceleration, Toyota Motor Sales USA's president said at the hearing. Source: http://www.businessweek.com/news/2010-05-25/toyota-sudden-acceleration-may-be-tied-to-89-deaths-update1-.html

**Toyota halts sales of Lexus LS flagship until parts arrive.** Toyota has stopped selling its flagship Lexus, the plush LS sedan, for about three weeks while it waits for parts to fix the car to reach dealers. A recall notice was issued on the LS Friday. Though the stoppage will not mean much to Toyota in terms of the number of LS cars it sells, the move is an enormous blow to its pride. The stoppage results from the recall Friday of about 3,800 LS models in the U.S., ranging from the LS 460 to the super-luxe LS 600h L, to fix the steering. Worldwide, the recall affects more than 11,000 cars. If a driver makes a sharp turn in the LS, the steering wheel may not return to its original position. "This is normal procedure if a (recall) remedy is not immediately available for a recall," a Toyota spokesman told Drive On. "Even if a remedy is available, dealers cannot sell a vehicle until the remedy is installed." The Associated Press said the missing parts are computer chips. This latest recall is unrelated to the record $16.4-million fine that Toyota paid after the Transportation Department faulted it for a slow response to safety deficiencies. The fine involved Toyota's troubles involving sticky accelerator pedals. Source: http://content.usatoday.com/communities/driveon/post/2010/05/toyota-halts-sales-of-lexus-ls-flagship-until-parts-arrive/1

## Emergency Services

**First responders seen still at risk from devices that can't talk to each other.** First responders remain at risk because their communications equipment too often cannot talk to other devices, a deadly problem for firefighters and police during the September 11 terror attacks, witnesses told Congress May 27. Consumer electronics continue to have higher interoperability standards. Mobile radios still sometimes don't communicate with other devices, even those made by the same manufacturers, a director at the Homeland Security Department, told the House science committee's technology

panel, He and a program manager at the National Institute of Standards and Technology, issued an "extremely urgent" call for action. They recommended test standards to ensure interoperability across vendors, townships and agencies. Source: http://content.usatoday.com/communities/ondeadline/post/2010/05/first-responders-called-still-at-risk-from-devices-that-cant-talk-to-each-other/1

**NASA develops new technology to enhance search and rescue operations.** NASA has developed new technology that will more quickly identify the locations of people in distress and reduce the risk of rescuers. The Search and Rescue Mission Office at NASA's Goddard Space Flight Center in Greenbelt, Md., in collaboration with several government agencies, has developed a next-generation search and rescue system, called the Distress Alerting Satellite System (DASS). NASA, the National Oceanic and Atmospheric Administration (NOAA), the U.S. Air Force, the U.S. Coast Guard and other agencies, are now completing the development and testing of the new system and expect to make it operational in the coming years after a complete constellation of DASS-equipped satellites is launched. When it goes online, DASS will be able to almost instantaneously detect and locate distress signals generated by 406 MHz beacons installed on aircraft and vessels or carried by individuals, greatly enhancing the international community's ability to rescue people in distress, said NASA's Search and Rescue Mission Manager. This improved capability is made possible because the satellite-based instruments used to relay the emergency signals will be installed on the U.S. military's Global Position System (GPS), a constellation of 24 spacecraft operating in mid-Earth orbit. Source: http://story.albuquerqueexpress.com/index.php/ct/9/cid/89d96798a39564bd/id/639250/cs/1/

## ENERGY

**President Obama to cancel offshore drilling projects.** A government administration official said that the U.S. President has canceled the August offshore drilling lease sale in the western Gulf of Mexico, and the lease sale off the coast of Virginia. The announcement comes as the President and his Administration face increased criticism for the failure of BP and the government to plug an oil well leak off the coast of Louisiana, and further contain the significant ecological damage to the region, and as the President prepared to travel to the Gulf for a second time Thursday. "The president's eyes have been opened" as to the risks of offshore drilling, a senior White House official told ABC News, in terms of the inability of the Minerals Management Service to reliably regulate the industry, and the inaccuracy of claims by the oil industry that companies are able to stop catastrophes like these from happening, and in the event that they do happen that the industry can contain the damage. Source: http://blogs.abcnews.com/politicalpunch/2010/05/president-obama-to-cancel-offshore-drilling-projects.html

**Restart of Alaska pipeline likely Friday.** The trans-Alaska pipeline remained shut down Wednesday, as responders took a cautious approach to cleaning up a crude oil spill confined to lined containment area. Up to several thousand barrels of crude oil spilled flowed May 25 during a scheduled pipeline shutdown at the pump station about 100 miles south of Fairbanks. The operator of the trans-Alaska pipeline system said oil should once again flow through the 800-mile line sometime Friday. Alyeska Pipeline Service Co. had hoped that the line — shut down since a spill earlier in the week — could be restarted by Thursday night, but officials said the process of coming back online has taken longer than expected. Source: http://www.wtop.com/?sid=1965719&nid=111

(Connecticut) **Thieves steal $60K in copper, police say.** Hartford, Connecticut police have blown the lid off a serious copper caper in the capitol city. Police said burglars broke into a Connecticut Light & Power facility in Hartford's Parkville neighborhood and made off with $60,000 in copper. According to police, the thieves made off with solid copper wire, bushings and breaker contacts. Even with a fence, burglars got into the building and caused damage to asbestos insulation and other materials causing more than $500,000 in damage. Hartford police, after getting tips from local businesses, have arrested three people in connection with the thefts and damage. CL&P has taken steps to make sure a similar incident does not happen again. The company began double-locking doors and placing plywood over first floor windows. Source: http://www.wfsb.com/news/23663248/detail.html

(Pennsylvania) **Easton man caught stealing copper from PPL, police say.** An Easton, Pennsylvania man is charged with trying to stealing more than $5,000 worth of copper from a Schuylkill County electric station, said state police in Frackville. The man is charged with theft, criminal conspiracy, criminal mischief, criminal trespass and possessing instruments of crime. He was sent to Schuylkill County Prison under $25,000 bail. According to court records, troopers came across the man and an unidentified man inside the station and said they were stealing items. Police said the man and his accomplice cut a hole in a fence to enter the station, and tried to steal tools and a large amount of copper cable valued at $5,500. Source: http://www.mcall.com/news/local/all-a21_mc-schuylkill-theft.7282317may23,0,2781361.story

## Food and Agriculture

**CDC identifies more sickened by alfalfa sprouts.** Federal officials have identified six additional cases of salmonella poisoning linked to raw alfalfa sprouts, bringing the total to 28 people sickened in 10 states. The Centers for Disease Control and Prevention said May 27 that three more people were sickened in California, for a total of 14 cases there. Caldwell Fresh Foods of Maywood, California, announced a nationwide recall of its alfalfa sprout the week of May 17. Other new cases were found in Arizona and Idaho. Nevada, Wisconsin, Oregon, Illinois, Missouri, New Mexico and Colorado also identified cases linked to the outbreak. The sprouts were sold to more than 400 Wal-Mart stores in 15 states. Salmonella can cause sometimes fatal infections in those with weakened immune systems. Source: http://www.google.com/hostednews/ap/article/ALeqM5hIZHk9HEfgKdIVkCFg-pxdjfF-xAD9FVHJL03

**Technique detects more than 700 antimicrobial-resistance genes.** Using an advanced genetic screening technique, Agricultural Research Service (ARS) scientists and cooperators have detected, for the first time, more than 700 genes that give microbes like Salmonella and E. coli the ability to resist antibiotics and other antimicrobial compounds. The researchers used what is called DNA microarray technology to find the resistance genes in a wide variety of bacteria such as Salmonella, E. coli, Campylobacter, Listeria, and Enterococcus, among others. These organisms can cause food poisoning and are thus a major public health concern. Researchers are concerned that some of these organisms have acquired genetic resistance to the antibiotics used to kill them. Finding the genes that confer resistance is an important step for scientists looking for new ways to control these organisms. All genes identified in organisms are logged into GenBank, a gene database administered by the National Center for Biotechnology Information at the National Institutes of Health. ARS microbiologists and collaborators at the Sidney Kimmel Cancer Center in San Diego, California, searched through GenBank for genes annotated by other scientists to likely encode resistance. This

work was published in the scientific journal Microbial Drug Resistance. Source: http://www.physorg.com/news194195231.html

**Honeybee death mystery deepens.** A one-two punch by a gut parasite and viruses may help explain the mysterious decline in U.S. honeybees seen over the last four years. Bees infected with both the fungal parasite Nosema ceranae and with any one of a handful of RNA viruses were much more likely to have come from hives on the decline than from healthy hives, researchers reported May 25 at a meeting of the American Society for Microbiology. The finding represents a new twist in a complex and multifaceted scientific problem, termed colony collapse disorder, made urgent by the continuing and severe losses suffered by U.S. beekeepers beginning in 2006. About a quarter of beekeepers have been affected, according to the Apiary Inspectors of America, an industry group. These beekeepers, including honey producers as well as many who lease out their bees to pollinate food crops, have reported losing between 30 and 90 percent of their hives. The latest nationwide survey, of 2009-2010 winter losses, revealed more than 30 percent of hives were lost for a variety of reasons. "We think that Nosema leaves the bees more open to infection by other organisms," said a bee researcher of the United States Department of Agriculture's Agricultural Research Service in Beltsville, Maryland, who presented the new results. "Our current thinking is that the Nosema parasite is a precursor to infectious diseases" that lead to colony collapse disorder. Source: http://www.usnews.com/science/articles/2010/05/28/honeybee-death-mystery-deepens.html

(California) **Fresh Express recalls romaine lettuce potentially contaminated with salmonella.** Another lettuce recall has been issued after salmonella poisoning was found in a package randomly tested by the Food and Drug Administration (FDA). Salinas, California-based Fresh Express issued a voluntary recall on several different ready-to-eat packages of salad mix. The packages all had use by dates of May 13 through May 16 and an "S" in the product code. The packages were distributed to 26 states in the North, West and Midwest. The Canadian Food Inspection Agency has issued a recall on the same products as well. Products involved in the recall include various salad-making kits, romaine lettuce, Caesar salad mix and various other mixes with romaine lettuce. Twenty-four different products produced by the company are included in the recall. Although, the packages are probably not available for sale in grocery stores because of the expired date, consumers who have the products in their refrigerators are asked to throw them away. There have been no reports of any illnesses related to these packages. The recall states the packages have the potential to contain salmonella. Source: http://www.techjackal.net/other/2010/05/26/fresh-express-recalls-romaine-lettuce-potentially-contaminated-with-salmonella/

**Scientist issues grasshopper alert.** A major infestation of grasshoppers may be in store for Wyoming, Montana, Nebraska and the Dakotas this summer, a grasshopper specialist said. The U.S. Department of Agriculture (USDA) expert on grasshopper suppression is warning that this summer could be the worst for grasshoppers since the mid-1980s, USA Today reported May 26. He said the threat assessment is based on the USDA's annual survey of adult grasshopper populations conducted each year in late summer. High numbers recorded last summer were part of a natural buildup of grasshopper populations, the USDA expert said. An entomologist with the Nevada Department of Agriculture said grasshoppers can wipe out farm crops and decimate fields of native grasses that feed cattle. "I've seen alfalfa fields where there's nothing left but stubble," the entomologist said. Federal and state officials can spray land with chemicals that would eventually kill the insects. Source:

http://www.upi.com/Science_News/2010/05/26/Scientist-issues-grasshopper-alert/UPI-92301274886267/

**FDA needs more clout to make food supply safer.** The Food and Drug Administration (FDA) needs more authority, more cooperation from other agencies and must do more scientific research to make the U.S. food supply safer, the General Accountability Office (GAO) said May 24. The FDA also must do more to help consumers navigate the maze of food supplements on the market and requires more power to regulate them, the GAO said. A series of food safety scares has shaken consumer confidence in the food supply, the GAO said. Just last week California-based Caldwell Fresh Foods recalled alfalfa sprouts after salmonella sickened 20 people. "We found that FDA was hampered in its ability to carry out some food safety responsibilities — oversight of food labels, fresh produce, and dietary supplements — because it lacked certain scientific information," the GAO's director of natural resources and environment said in a letter accompanying the report. The GAO, the investigative arm of Congress, said the FDA had tried to meet some of its recommendations but needed to do more. "First, imported food makes up a substantial and growing portion of the U.S. food supply, with 60 percent of fresh fruits and vegetables and 80 percent of seafood coming from across our borders," it said. The FDA can inspect just 1 percent of this food. "Second, we are increasingly eating foods that are consumed raw and that have often been associated with foodborne illness outbreaks, including leafy greens such as spinach." The FDA regulates 80 percent of the food supply, except for meat and processed egg products, which the U.S. Department of Agriculture regulates. Source: http://www.reuters.com/article/idUSTRE64N5UZ20100524

*May 27, Associated Press* – (National) **Businesses could use U.S. cyber monitoring system.** A U.S. government computer security system that can detect and prevent cyber attacks should be extended to private businesses that operate critical utilities and financial services, a top Pentagon official said May 26. The Deputy Defense Secretary said discussions are in the very early stages and participation in the program would be voluntary. The idea, he said, would allow businesses to take advantage of the Einstein 2 and Einstein 3 defensive technologies that are being developed to put in place on government computer networks. Extending the program to the private sector raises a myriad of legal, policy and privacy questions, including how it would work and what information, if any, companies would share with the government about any attacks or intrusions they detect. Businesses that opt not the participate could "stay in the wild, wild west of the unprotected Internet," the secretary told a small group of reporters during a cybersecurity conference. And in the case of Einstein 2 — an automated system that monitors federal Internet and e-mail traffic for malicious activity — companies already may have equal or superior protections on their networks. Source: http://www.google.com/hostednews/ap/article/ALeqM5iW7V4eoQIIMmdNQyzEdsPaiCWOuQD9FUQ8IG0

**Ranchers now fear return of fever ticks.** U.S. Department of Agriculture (USDA) fever-tick inspectors have become the latest set of American workers pulled from northern Mexico amid ongoing drug cartel violence, a move some Texas ranchers fear will reintroduce a pest that nearly wiped out U.S. cattle a century ago. Citing safety concerns, the department's Animal & Plant Health Inspection Service March 29 suspended its cattle inspections in Reynosa and Nuevo Laredo, Mexico. The agency last week diverted Reynosa inspections to nearby Pharr, Texas and this week opened a second U.S. facility in Laredo. A USDA spokeswoman said the agency is taking precautions to minimize the risk of a reinfestation. The non-native fever ticks transmit a blood parasite that causes bovine babesiosis, otherwise known as "Texas fever" or "cattle fever." The disease in the early 1900s spread through herds and wiped out nearly 90 percent of the cattle in some areas, helping end the era of cattle

drives to the north. In 2006, the USDA marked the 100-year anniversary of its successful Cattle Fever Tick Eradication Program, which by 1943 had eliminated the ticks in the United States except for a narrow quarantine zone along the border. The ticks in 2007 turned up beyond the quarantine zone, prompting a cry for more federal resources. There's growing concern about deer and other animals, such as non-native nilgai kept as exotic game for hunters, spreading the tick as they jump fences between ranches. A large part of the program has been done in Mexico, where the USDA has had 43 employees at 11 Mexican cattle inspection ports examining about a million head a year. About 38,000 of these come through Laredo, another 39,000 through Pharr. While the Laredo facility is outside the quarantine zone, a USDA spokeswoman said precautions were being taken to ensure ticks don't drop onto U.S. soil. Mexican agriculture inspectors are doing visual inspections before the cattle cross, she said, which makes for a "double inspection." Trucks are sealed by Mexican authorities and not unsealed until they get to the inspection facilities in Texas. Source: http://www.mysanantonio.com/news/mexico/usda_cattle_inspectors_pulled_from_mexico_94624674.html?showFullArticle=y

**Large amount of Ivermectin found in cans of corned beef.** Caribbean food products maker Grace Foods USA reported May 22 that canned corned beef distributed in the United States contains higher than acceptable levels of a Ivermectin, which is used to treat cattle for parasites. Ivermectin can make people sick if they consume it. The recall of two batches of corned beef is based on an advisory from Grace Foods' Brazilian supplier. The supplier gave the warning after testing showed higher levels of Ivermectin than the U.S. Department of Agriculture allows. The 12-ounce cans of beef have codes 100204 or 100205 with "Brasil Inspecionado 337 S. I. F." stamped on the top. Source: http://topnews.us/content/220399-large-amount-ivermectin-found-cans-corned-beef

**Huge grasshopper outbreak projected in Northwest.** The Pacific Northwest must prepare for the worst grasshopper outbreak in 30 years, according to Washington State University and United States Department of Agriculture scientists. Researchers found a big increase in the number of grasshopper eggs last fall and said a relatively mild spring has set the stage for a major grasshopper infestation. Last summer, grasshoppers wiped out 7,000 acres of grassland in the high desert of southeastern Oregon. The areas considered at most risk in Washington are the high desert regions near Othello, Yakima and the Tri-Cities. The infestation was expected to hit its peak in late July and early August. Federal officials are looking into pesticide options. "In some areas there will indeed be masses," said a WSU entomologist. "Not biblical proportions, but big masses of grasshoppers moving through areas." Grasshoppers can travel from 30 to 50 miles a day looking for food. Scientists are also warning of a possible outbreak of the "Mormon Cricket," an insect that doesn't fly, but travels in tight packs and devours everything in its path. "There are massive numbers of them, and then when they exit that area, pretty much anything green is gone," said the WSU entomologist. Source: http://www.fosters.com/apps/pbcs.dll/article?AID=/20100524/GJLIFESTYLES/100529884/-1/SANNEWS

## Government Sector (including Schools and Universities)

(Wisconsin) **Rock County Courthouse evacuated amid bomb threat.** Authorities closed the Rock County, Wisconsin, Courthouse Friday morning after a bomb threat was made. Rock County sheriff's

deputies were dispatched to the courthouse at about 7:50 a.m. The threat was apparently called into the clerk of courts office. The building has been evacuated and is temporarily closed to the public. Authorities said that they are conducting a search of the building. Rock County sheriff's detectives are coordinating the investigation. Law enforcement officials are asking members of the public to avoid the courthouse area. Source: http://www.channel3000.com/news/23707978/detail.html

(Ohio) **Bomb squad called to Youngstown City Hall.** Youngstown (Ohio) City Hall was evacuated, just before it was set to close for the day Tuesday, when a suspicious package was delivered to the clerk of court's Office. The Youngstown Bomb Squad was called in to investigate, and a portion of West Boardman Street was blocked to traffic as a pre-caution until police could examine the package that was sent from Damascus, Syria and delivered by a service not normally used by city hall. The Youngstown clerk of courts, said "we just received a suspicious package and it wasn't accurately addressed, but it did have the P.O. box and someone hand written it. It was delivered by a DHL person who alarmed my clerk, who brought it to me and indicated that it was suspicious." The Youngstown Bomb Squad commander said that the Youngstown clerk of courts did everything right. He said she treated it as a suspicious package and the bomb squad felt the same way. He said they used their procedures until they were sure that everything was okay. It took just under an hour for the bomb squad to investigate. They said the package was legitimate. Source: http://www.wfmj.com/Global/story.asp?S=12542847

(Colorado) **City of Denver Web site hacked again.** The Web site for the city and county of Denver has been hacked for the second time in a week. The Web site Denvergov.org was pulled down Monday night after a hacker replaced the city's home page with a green and black page, and the Web site said it was still down for maintenance Tuesday morning. Denvergov.org also was hacked May 20 and was down for about six hours. A mayor's office spokesman said Monday he didn't know whether the cases were related. Denver police are investigating both cases. Source: http://cbs4denver.com/wireapnewsco/City.of.Denver.2.1713457.html

(Texas) **School officials evacuate Cove High over bomb threat.** Emergency vehicles arrived at Copperas Cove High School in Texas before noon Monday, after an anonymous caller phoned in a bomb threat that led administrators to evacuate the school. Copperas Cove police searched the school while students, faculty and staff waited outside for about 90 minutes in the midday heat. Police found no sign of a bomb, and students and teachers were allowed to re-enter the building around 1:30 p.m. for the remainder of the school day. A Copperas Cove police spokesman said police are still investigating who called in the threat, which is a serious crime. The call is a state jail felony because it involved a school, he said. Additionally, whoever is responsible will be liable for costs incurred by the district and by emergency officials during the incident. Source: http://www.kdhnews.com/news/story.aspx?s=41744

(Indiana) **Ind. fed building evacuated after powder found.** The federal building in downtown Evansville, Indiana was evacuated because of a report of white powder found in an envelope. Evansville Fire Department's hazardous materials team is investigating after the Monday afternoon evacuation. The district chief said the substance was taken from the building for testing. The building was evacuated as firefighters collected the powder, isolated the envelope and cleaned the area. The worker who found the powder was told to take a shower as a precaution. The district chief declined to comment on who the envelope was addressed to or whether it included a return address.

Firefighters on the scene said many of the workers in the downtown Evansville building went home for the day after the building was evacuated. Source: http://www.chicagotribune.com/news/chi-ap-in-federalbuilding-p,0,7474765.story

(Wisconsin) **Explosive devices locks down Milwaukee high school.** Milwaukee Police said Tuesday that they have arrested 2 students on felony charges after a lockdown at Riverside High School. Police said the arrests stem from the discovery of homemade explosive devices placed around the school, Monday. Police said one of the devices actually exploded, but there were no injuries. Police are not elaborating about the devices, but a Milwaukee schools spokeswoman said the devices were not hazardous and were made from bottles. School staff noticed that the bottles, which had been placed around the school, were foaming. The all-clear was given and students were dismissed as scheduled at 2:40 p.m. Source: http://www.wqow.com/Global/story.asp?S=12537218

(Kansas) **Courthouse evacuated due to suspicious package.** The Leavenworth County Courthouse in Kansas was evacuated for about an hour May 21 as authorities investigated a suspicious bag. Employees were allowed back into the building after it was determined the bag contained only personal hygiene products, according to law enforcement officials. The incident was reported at about 11:15 a.m. when an employee saw someone put down the bag but then lost sight of the person. The bag had been left in the area of the county treasurer's office. The bomb squad X-rayed the bag and found nothing associated with a hazardous device; rather, it was described as a shaving kit. Source: http://www.leavenworthtimes.com/homepage/x1560873936/Courthouse-evacuated-due-to-suspicious-package

## Information Technology and Telecommunications

**Hackers will keep hammering Facebook, say researchers.** Attacks targeting Facebook users will continue, and they could easily become even more dangerous, a security researcher said today. Over the last two weekends, cybercriminals have launched large-scale attacks using rogue Facebook applications that infect users of the popular social networking site with adware that puts pop-ups on their screens. "There are limitations to what Facebook can do to stop this," said a U.K.-based researcher for Websense Security Labs. "I wouldn't be surprised to see another attack this weekend. Clearly, they work." According to the chief technology officer at antivirus vendor AVG Technologies, last weekend's attack was about half the size of the one the weekend before. Both featured messages that used sex-oriented videos as bait to convince users to install a Facebook application and then download a purported update to a free video player program. The download was actually adware. Both researchers agree that the attacks would keep coming. The hackers are "trying to make money and looking for ways to 'work' Facebook," said one of the researchers in an instant message. Source:
http://www.computerworld.com/s/article/9177436/Hackers_will_keep_hammering_Facebook_say_researchers

**Businesses could use U.S. cyber monitoring system.** A U.S. government computer security system that can detect and prevent cyber attacks should be extended to private businesses that operate critical utilities and financial services, a top Pentagon official said May 26. The Deputy Defense Secretary said discussions are in the very early stages and participation in the program would be voluntary. The idea, he said, would allow businesses to take advantage of the Einstein 2 and Einstein

3 defensive technologies that are being developed to put in place on government computer networks. Extending the program to the private sector raises a myriad of legal, policy and privacy questions, including how it would work and what information, if any, companies would share with the government about any attacks or intrusions they detect. Businesses that opt not the participate could "stay in the wild, wild west of the unprotected Internet," the secretary told a small group of reporters during a cybersecurity conference. And in the case of Einstein 2 — an automated system that monitors federal Internet and e-mail traffic for malicious activity — companies already may have equal or superior protections on their networks. Source: http://www.google.com/hostednews/ap/article/ALeqM5iW7V4eoQIIMmdNQyzEdsPaiCWOuQD9FUQ8IG0

**Europe warns Google, Microsoft, others about search-data retention.** Google, Microsoft, and Yahoo are retaining detailed search engine data for too long and not making it sufficiently anonymous later, in violation of European law, the European Union's data-protection advisory body has warned. The three companies received letters May 26 from the Article 29 Data Protection Working Party, which oversees data-protection issues in the E.U. Since 2008 the working party has pressured search companies to retain highly detailed search records for no longer than six months. Google, Yahoo, and Microsoft all agreed to modify how long they store the detailed data, which varied up to 18 months. The data collected by search engines can include a host of details, including the search terms, the date and time of the search, the searcher's IP (Internet Protocol) address and the brand of browser, operating system and language used. Google keeps the full data for nine months and then obscures the last octet of the IP address. The working party wrote to Google stating that that policy does not protect the "identifiability of data subjects." Also, Google retains cookies — data files used to track how a person moves around a Web site — for 18 months, which would also allow for the correlation of search queries, the working party said. In a news release, the working party singled out Google, saying that that company's 95 percent market share in some European countries means it "has a significant role in European citizens' daily lives." Source: http://www.computerworld.com/s/article/9177424/Europe_warns_Google_Microsoft_others_about_search_data_retention

**Cisco bugs surrender control of building's critical systems.** Cisco Systems has warned of serious vulnerabilities in a device that connects a building's ventilation, lighting, security, and energy supply systems so they can be controlled by IT workers remotely. The networking giant May 26 urged users of the Cisco Network Building Mediator products to patch the vulnerabilities, which among other things allow adversaries to obtain administrative passwords. No authentication is required to read the system configuration files, making it possible for outsiders to take control of a building's most critical control systems. "Successful exploitation of any of these vulnerabilities could result in a malicious user taking complete control over an affected device," a Cisco advisory stated. The notice also warned that the vulnerabilities are present in the legacy products from Richards-Zeta, the Cisco-acquired company that originally designed the system. The bugs were discovered during internal testing. Another flaw makes it possible for low-level employees to gain full control of the device by accessing default administrative accounts. Other bugs allowed malicious insiders to intercept traffic as it travels between an administrator and the building mediator and to escalate limited privileges. Source: http://www.theregister.co.uk/2010/05/26/cisco_building_control_bugs/

**DHS official stresses cybersecurity is industry's responsibility.** Contractors that fail to live up to security requirements in federal technology contracts should be held accountable, even if the vulnerabilities originated in products or capabilities provided by suppliers, a top Homeland Security Department (DHS) official said May 25. In most business situations, "if we have a contractual arrangement and you fail [to meet the requirements], I have legal recourse," said the director of global cybersecurity management at DHS. "Why wouldn't the same be true when the supply chain [is involved]? I'm buying a product from you, and you represent that it's a product with the following characteristics. If you fail, I have a right to sue you." The director spoke at the SecureAmericas conference in Arlington, Virginia, an event hosted by the cybersecurity provider International Information Systems Security Certification Consortium. He noted a number of examples where failures in the supply chain led to serious security implications, including a wave of hard drives infected with viruses that infiltrated the U.S. market from Asia in 2007 and a recent case in which thumb drives were shipped preinstalled with malicious software, eventually leading to the Defense Department imposing a temporary ban on the storage devices. Source: http://www.nextgov.com/nextgov/ng_20100525_8667.php

**Default database passwords still in use.** The rampant use of default passwords within live database environments continues to plague the security of enterprise data, researchers said. "It's a problem that has been around for a long, long time," said the manager of Team SHATTER, Application Security Inc.'s research arm. "A lot of default passwords out there get installed when you deploy a database, you install an add-on to it, or even if you install a third-party application that uses the database." As he puts it, the problem of default passwords lingering in the wild has built up during the years as a result of cumulative errors by both vendors and database administrators. In the past, the majority of vendors had no compunction about pushing out installers that automatically created default accounts to expedite the deployment of new databases, add-ons, or applications on top of the database. Users did nothing to clean up these default accounts once installation was complete. The manager said the situation on the vendor front has improved considerably in recent years, but default passwords continue to be a problem for a number of reasons. To date, AppSec's team has collected more than 1,000 well-known default user name and password combinations used by different vendors within databases across the IT spectrum. Organizations should do a thorough check of their database accounts to ensure they are not using any of the combos on the list. Source: http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=225200102&subSection=Application+Security

**Spam and viruses see minor rises, as 9 out of 10 spam e-mails have a hyperlink or URL contained in the message.** In the May 2010 Symantec MessageLabs Intelligence Report, analysis has revealed that nine out of 10 spam e-mails now contain a URL link in the message and in May, 5 percent of all domains found in spam URLs belonged to genuine Web sites. Of the most frequently used domain names contained in spam URLs, the top four belong to well-known Web sites used for social networking, blogging and file sharing and host other forms of user-generated content. The report also found that there was a minor increase by 0.3 percent of spam in e-mail traffic, while analysis of Web security activity showed that 12.4 percent of all Web-based malware intercepted was new in May, an increase of 1.5 percent since April. MessageLabs Intelligence also identified an average of 1,770 new Web sites per day harbouring malware and other potentially unwanted programs such as spyware and adware, an increase of 5.6 percent since April. Source: http://www.scmagazineuk.com/spam-

and-viruses-see-minor-rises-as-nine-out-of-ten-spam-emails-have-a-hyperlink-or-url-contained-in-the-message/article/171011/

**Business continuity, not data breaches, among top concerns for tech firms.** Data security and breach prevention ranks low as a risk factor for most big technical companies, according to new research that identifies the most widespread concerns among the 100 largest U.S. public technology companies. The research, released by BDO, a professional services firm, examines the risk factors listed in the fiscal year 2009 10-K SEC filings of the companies; the factors were analyzed and ranked in order by frequency cited. Among security risks, natural disasters, wars, conflicts and terrorist attacks were cited by 55 percent of respondents as a risk concern and was 16th on the list, much higher than breaches of technology security, privacy and theft, which was mentioned by 44 percent of the companies, putting it at 23rd on the list. The leader of the Technology Practice at BDO said he thought business continuity was driving worries about risks like natural disasters and conflicts. Accounting, internal controls and Sarbanes-Oxley compliance is the 18th largest risk factor this year, according to the list. Source: http://www.computerworld.com/s/article/9177262/Business_continuity_not_data_breaches_among_top_concerns_for_tech_firms

**Apple Safari 'carpet bomb' flaw remains unfixed two years later.** Apple fixed the so-called "carpet bomb" vulnerability in its Safari browser for Windows after Microsoft issued a security advisory about it in July 2008, but to date the very same flaw in Safari for OS X is still unpatched. The security researcher who alerted Apple of the flaw in May 2008 said the threat of an attacker exploiting this bug is alive and well today, especially with the growth in popularity of Safari and OS X. He said in 2008 Apple told him it did not consider the issue a security vulnerability but more of a design issue, and that it did not have plans to fix it anytime soon. The researcher said the vulnerability could let a bad guy download malicious binaries and data files into the browser's downloads folder without the user knowing because Safari does not ask the user whether he wants to save the file on his machine, which most other browsers do. So when a user visits a malicious Web site, Safari would allow the site to download files without prompting the user. The main threat the flaw poses is a denial-of-service attack on the victim's machine. The carpet bomb DoS attack would wipe out a session and "whatever you were working on would be gone," the researcher said. Source: http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=225200002

**Researcher finds new type of phishing attack.** A researcher has found a new method for carrying out phishing attacks "that takes advantage of the way that browsers handle tabbed browsing and enables an attacker to use a script running in one tab to completely change the content in another tab," according to ThreatPost. The attack, discovered by a researcher for Mozilla, relies on users visiting a controlled infected Web site. When the user visits the infected Web site, it reads what other tabs the user has opened in the browser and changes itself to look like a selected page. The researcher actually demonstrates it on his Web site in which the page alters to appear as the log-in page for Google. The system could also be used in the case of banking Web sites, etc. to steal login and account information. Source: http://www.thenewnewinternet.com/2010/05/25/researcher-finds-new-type-of-phishing-attack/

**Iranian cyber army second largest in the world, claims Iranian commander.** After hacking Twitter and various Iranian Web sites and engaging in a cyber war with China, the Iranian Cyber Army is said to be looking at the Revolutionary Guards for direction, according to a senior Revolutionary Guards Corps commander. Fars news agency reports that the commander of the Ali Ebn-e Abi Taleb Guards in Qom, said May 20 that the Revolutionary Guards has been successful in establishing a cyber army and "today the cyber army of the Revolutionary Guards is the second largest cyber army in the world." The commander also claimed the objective of the Iranian Cyber Army is "to prevent the destruction of Iran's cultural and social system" and added the "cyber army of the Revolutionary Guards is a force to reckon with in this arena." The Iranian Cyber Army has not been officially claimed by any group. Last year, Defense Tech, a U.S. military and security organization announced that the Iranian Cyber Army belongs to the Revolutionary Guards of Iran. Source: http://www.thenewnewinternet.com/2010/05/21/iranian-cyber-army-second-largest-in-the-world-claims-iranian-commander/

**New threat for wireless networks: Typhoid adware.** There is a potential threat lurking in your Internet cafe, say University of Calgary computer science researchers: Typhoid adware. Typhoid adware works in similar fashion to Typhoid Mary, the first identified healthy carrier of typhoid fever who spread the disease to dozens of people in the New York area in the early 1900s. "We're looking at a different variant of adware — Typhoid adware — which we have not seen out there yet, but we believe could be a threat soon," said an associate professor who co-authored a research paper with a assistant professor and two students. Typhoid adware could be spread via a wireless Internet cafe or other area where users share a nonencrypted wireless connection. Typically, adware authors install their software on as many machines as possible. But Typhoid adware hijacks the wireless access point and convinces other laptops to communicate with it instead. Then the Typhoid adware automatically inserts advertisements in videos and Web pages on hijacked computers, the researchers said. Meanwhile, the carrier sips her latte in peace — she sees no advertisements and doesn't know she is infected, just like symptomless Typhoid Mary. Source: http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=224900741&subSection=End+user/client+security

**Bugnets could spy on you via mobile devices.** Imagine an individual sitting in a cafÃ© discussing the details of a business proposal with a potential client. Neither the individual nor the client has a laptop; they are just two people having a conversation. But unbeknownst to either, someone half a world away is listening to every word they say. Later, as the individual leaves, they receive a text message referring to the proposal and demanding money in exchange for silence. Recent research from two universities suggests that such a remote-eavesdropping scenario may soon be possible. According to two George Mason University researchers, cell phones make excellent surveillance devices for remote snoops. In a paper, both discuss a "modernized mic hijacker" that an attacker could control over what they call a "roving bugnet." The eavesdropper would use a piece of malware called a "bugbot" to listen in on in-person interactions via a nearby smartphone or laptop. Such attacks would be more likely to target specific people (a wayward spouse, say) than to play a role in widespread attacks on the general public. Source: http://www.networkworld.com/news/2010/052310-bugnets-could-spy-on-you.html?hpg1=bn

**Facebook users suffer second 'sexy' malware attack.** Security experts have called on Facebook to set up an early warning system on its network to notify users of any threats and when they occur, after yet another malware attack hit the site over the weekend. The attack is the second in successive Saturdays to use a "sexy video" to lure the recipient into clicking on a fake FLV Player upgrade message, which then downloads adware onto the PC. Both files arrive as a thumbnail video in messages posted to users' walls. Last week's included the message: "This is without doubt the sexiest video ever!: P :P :P.," while the new scam refers to "distracting beach babes." Facebook is aware of the problem and is "actively removing both the wall posts and the malicious applications," wrote a Websense senior research manager in a blog post. Source: http://www.v3.co.uk/v3/news/2263552/facebook-suffers-second-sexy

**Google introduces SSL encrypted search engine, as Hotmail moves to protect users further.** Google has added full SSL encryption to its search services to allow users to have a secure https connection when searching google.com. The page is accessed by specifically entering https://www.google.com/ in the address bar. A Google software engineer claimed that by adding SSL encryption to products including Gmail to Google Docs, the session-wide encryption was "a significant privacy advantage over systems that only encrypt login pages and credit card information." Google also clarified that the release is in beta to cover only the core Google Web search product, and not on Image Search and Maps. Since SSL connections require additional time to set up the encryption between the browser and the remote Web server, a user experience with search over SSL may be slightly slower than a regular Google search experience. Google also claimed that it will still maintain search data "to improve your search quality and to provide better service." Source: http://www.scmagazineuk.com/google-introduces-ssl-encrypted-search-engine-as-hotmail-moves-to-protect-users-further/article/170796/

## National Monuments and Icons

**BP Oil Spill: 15 National parks in grave jeopardy.** From Padre Island National Seashore in Texas to the Everglades National Park in Florida, the 15 national parks, wildlife refuges and state parks in Gulf states most threatened by the ongoing BP oil blowout are identified in a new report from the Natural Resources Defense Council (NRDC) and the Rocky Mountain Climate Organization (RMCO). The new NRDC/RMCO report, "Special Places at Risk in the Gulf: Effects of the BP Oil Catastrophe," lists national and state parks and wildlife areas in Florida, Louisiana, Texas, Alabama, and Mississippi at risk to contamination because of the BP oil blowout. The list was chosen to include the best examples of the full range of both the protected coastal public areas and the resources within them that are vulnerable to contamination by the BP disaster. Because the potential reach of this catastrophe is so broad, our list certainly cannot include more than a tiny fraction of what is at stake as oil continues to gush into and spread around the Gulf. But by highlighting some of these special places and what they protect, this report may shed some light on the amazing environment of the Gulf of Mexico that now threatened by the BP oil disaster. Source: http://www.providingnews.com/bp-oil-spill-15-national-parks-in-grave-jeopardy.html

(New Mexico) **New Fire: 16,201 acres burnt; 40 percent contained.** The New Fire in the backcountry area of Carlsbad Caverns National Park in New Mexico is now 40 percent contained after burning 16,201 acres. That acreage breaks down to 12,976 acres of National Park Service land, 2,681 Bureau of Land Management land and 364 acres of state land. Vegetation in the New Fire area is mostly a

mixture of grass and shrubs. The 450-acre Yucca Fire has remained inactive for several days. The fires are being managed by New Mexico Southwest Type II Incident Management Team (Cowie IC). There have been three minor injuries among the 450 total personnel fighting the fire. Estimated costs to date have reached $1,597,106. Park status remains much the same. The main cave at the caverns is open for visitors. The scenic loop drive, called Walnut Canyon Desert Drive, reopened May 26. All backcountry trails remain closed for public safety due to fire activity. Source: http://www.currentargus.com/ci_15170008

## Postal and Shipping

Nothing Significant to Report

## Public Health

**FDA says diet drug can cause liver damage.** The Food and Drug Administration (FDA) is warning of rare instances of liver injury in some people talking the popular weight-loss drug orlistat. The drug is marketed under the brand names Xenical and Alli. The former is only sold over-the-counter. The agency has approved a revised label for Xenical that states the liver-injury risk, according to an agency statement. The brand contains 120 milligrams of orlistat. Alli has 60 milligrams. The FDA has identified 13 cases of severe liver injury associated with orlistat, only one of which occurred in the United States. Symptoms of liver damage include itching, yellow eyes or skin, dark urine, loss of appetite and light-colored stools. Source: http://www.allheadlinenews.com/articles/7018830419

(New York) **Experimental drug boosts cure rate for Hepatitis C.** A new drug under development for Hepatitis C greatly improved the cure rate for patients while cutting the time needed for treatment, according to the drug's maker, Vertex Pharmaceuticals. As reported by The New York Times, about 75 percent of patients enrolled in the trial who took the drug, telaprevir, along with standard treatment, essentially rid themselves of the virus, which can lead to liver damage and even cancer. In comparison, just 44 percent of patients who took the standard therapy alone had the same results. Telaprevir works by blocking a protease, an enzyme manufactured by the virus, similar to how powerful HIV medications attack that pathogen. Source: http://www.businessweek.com/lifestyle/content/healthday/639508.html

**New way bacterium spreads in hospital.** Health care workers and patients have yet another source of hospital-acquired infection to worry about, British researchers are reporting. Clostridium difficile, a germ that causes deadly intestinal infections in hospital patients, has long been thought to be spread only by contact with contaminated surfaces. But a new study finds that it can also travel through the air. The researchers emphasized that there is no evidence that C. difficile can be contracted by inhaling the germs. Rather, they float on the air, landing in places where more people can touch them. The bug is commonly spread by contact with infected feces, and the British scientists said the new study made it even more urgent to isolate hospital patients with diarrhea as soon as possible — even before tests confirm a C. difficile infection. Outbreaks of C. difficile, a bacterium resistant to many antibiotics, have been increasing in the United States since 2001, along with the evolution of more virulent strains. Source: http://www.nytimes.com/2010/05/25/health/25infect.html

(Illinois) **Tuberculosis outbreak may push Kane Co. to dip into savings.** An outbreak of tuberculosis at a homeless shelter in Aurora, Illinois might now result in Kane County spending an additional $65,000 to prevent the problem from getting worse. The outbreak was first spotted several months ago at Hesed House. Since then, 13 people exposed to the bacteria at the shelter have developed the active form of the infection. Homeless people tend to live a high-stress lifestyle that wears on their immune system, making them more susceptible to tuberculosis, said the executive director of the Kane County Health Department. He appeared before the county's public health committee Tuesday to plead for more money to stop the outbreak from spreading through the homeless population and among the general public. Tuberculosis can be lethal if left untreated. Source: http://www.dailyherald.com/story/?id=383417

**New threats to U.S. blood supply.** Public health officials are battling a host of new infectious threats to the nation's blood supply. Blood centers, which have long tested for risks like hepatitis C and AIDS, have added a number of new tests on donated blood in recent years, including checks for West Nile virus and Chagas, a tropical parasitic disease. But new screening tests are hard to develop and can take years to win government approval. Currently, for instance, there's no way to screen for newer threats like babesiosis, a parasitic infection that has been linked to 10 U.S. deaths through blood transfusions since 2006. And a dangerous virus known as Chikungunya has spread to the U.S. and Europe from Africa in the last several years. Blood supply officials are urging the U.S. government to adopt so-called pathogen-reduction technology that can kill a wide range of contaminants in blood after it has been donated. One method already in use in about a dozen countries in Europe, Asia and elsewhere destroys most pathogens with a combination of chemicals and ultraviolet light. The Food and Drug Administration declined to approve the technology several years ago, citing possible side effects. But the agency is continuing to evaluate it. Source: http://online.wsj.com/article/SB10001424052748704792104575264600619273586.html?mod=WSJhpp_MIDDLENexttoWhatsNewsFifth

**Tylenol maker pledges quality overhaul.** Drugmaker McNeil Consumer Healthcare, currently under investigation by the Food and Drug Administration following a string of recalls related to its over-the-counter drugs including Tylenol, Motrin and Benadryl, outlined steps Tuesday to remedy serious quality and safety lapses at its manufacturing facilities. McNeil, a division of Johnson & Johnson, has initiated four recalls of its products in the past seven months, including a widespread recall of children's non-prescription drugs May 1. Johnson & Johnson has suspended production at McNeil's Fort Washington, Pennsylvania plant that manufactured the children's products. Johnson & Johnson also faces Congressional hearings Thursday about McNeil's product recalls. Among the measures, the drugmaker said it has hired an independent pharmaceutical consulting firm to identify corrective actions to improve quality and manufacturing systems at its Fort Washington facility. The company said it is improving employee training in every part of the manufacturing and quality operations, and implementing new processes for conducting investigations on quality levels. McNeil also said the company has made significant organizational changes but did not provide details about the changes. Source: http://money.cnn.com/2010/05/25/news/companies/tylenol_recall_mcneil_quality_overhaul/

**U.S. government stockpiles new, safer smallpox vaccine.** The U.S. government has begun bolstering its smallpox vaccine stockpile with a new version designed to close a gap that left millions vulnerable to a bioterror attack. The vaccine, Denmark-based Bavarian Nordic's Imvamune, is made with

modified vaccinia ankara, a safer alternative to the cowpox vaccines used for generations. Company officials said the first shipments arrived in the U.S. Strategic National Stockpile last week, within hours of a World Health Organization ceremony marking eradication of the disease, widely regarded as one of the great public health achievements of all time. Source: http://www.usatoday.com/news/health/2010-05-25-smallpox25_ST_N.htm?csp=34news

**FDA approves swine flu test for permanent use.** The Food and Drug Administration (FDA) said it has approved the first diagnostic test for 2009 swine flu under its traditional approval system. The FDA previously cleared several tests on a limited basis for use during the declared public health emergency related to swine flu. The new Simplexa Influenza test from Focus Diagnostics in Cypress, Calif., uses specimens from nasal swabs to detect the H1N1 virus. The director of the FDA's center for devices, said the FDA clearance means the availability of the Simplexa H1N1 test will not be affected when the public health emergency expires. The federal government estimates between 43 and 88 million cases of swine flu occurred between April last year and March 2010. Source: http://www.google.com/hostednews/ap/article/ALeqM5jIeY57u52O8NNTHIL-3pixdrLQXAD9FT9VL02

## Transportation

(Virginia) **NTSB develops helicopter-accident course.** The National Transportation Safety Board (NTSB) will host a five-day course in August focusing on rotorcraft accident investigation. The class — set for Aug. 16 to 20 at the NTSB Training Center in Ashburn, Va. — is designed to give investigators from regulatory agencies, private industry and other organizations the tools, methods and skills to conduct helicopter-related accident inquiries. The course will also examine case studies, including in-flight fires and break-ups, midair collisions and weather-related incidents. Source: http://www.aviationtoday.com/rw/topstories/NTSB-Develops-Helicopter-Accident-Course_68532.html

**Fat people barred from airplane exit rows.** Can overweight people sit in an airplane's exit row? Not if they're flying on Southwest, Alaska Airlines or AirTran and also need a seat-belt extender. But on American, United, Delta and Continental Airlines, one can have as many seat-belt extenders as he wants and still sit in the exit row. The Federal Aviation Administration set minimal standards for sitting in an exit row back in 1990: One must be at least 15-years-old, be able to follow the airline crew's directions, and be capable of opening the exit door, which equates to pushing around 50 pounds of weight. But the agency left it up to the airlines to develop their own exact exit row seating rules. "The reason behind the policy is safety,'' a Southwest Airlines spokeswoman said in an e-mailed statement. "It supports our ability to assist passengers in exiting the aircraft in an expeditious manner in the event of an emergency." Alaska Airlines, which has the same rule, gave a more detailed explanation. A spokeswoman said that the seat-belt extender creates a potential safety hazard. "With an extender, a seat belt can stretch across the floor and could become a tripping hazard for people exiting through the emergency exits." Source: http://www.dailyfinance.com/story/company-news/fat-people-airplane-exit-rows/19488271/

## Water and Dams

**Discovery may lead to safer drinking water, cheaper medicine.** A discovery that may pave the way to helping reduce health hazards such as E. coli in water could also make chemicals and drugs such as

insulin cheaper to produce and their production more environmentally friendly. By creating a three-dimensional model, a biochemistry professor and a post-doctoral student at Queen's University in Ontario, Canada discovered exactly how the AceK protein acts as a switch in some bacteria to bypass the energy-producing cycle that allows bacteria like E. coli and salmonella to go into a survival mode and adapt to low-nutrient environments, such as water. The unique feature of this discovery is that the switching on and off take place in the same location of the protein. Normally these two opposing activities would happen in two different active sites. "From a protein function point of view, this is unique and has never been discovered anywhere else," said the professor. The discovery opens the door for scientists to identify a molecule that can keep the bypass switch from turning on so bacteria will die in water. As a result, drinking water would be cleaner and the incident of water bacterial contamination, such as the Walkerton tragedy, could be reduced. Source: http://www.queensu.ca/news/articles/discovery-may-lead-safer-drinking-water-cheaper-medicine

**Wellwater contamination a health risk for more than one third of U.S. population say USGS scientists.** What's your poison? That question may be more appropriate when asking for a glass of water than bellying up to the bar with a friend. Maybe you would like a chemical cocktail of contaminants? About 105 million people — or more than one-third of the nation's population — receive their drinking water from one of the 140,000 public water systems across the United States that rely on groundwater pumped from public wells. More than 20 percent of untreated water samples from 932 public wells across the nation contained at least one contaminant at levels of potential health concern, according to a new study by the U.S. Geological Survey. The USGS focused primarily on source (untreated) water collected from public wells before treatment or blending, rather than the finished (treated) drinking water that water utilities deliver to their customers. Findings showed that naturally occurring contaminants, such as radon and arsenic, accounted for about three-quarters of contaminant concentrations greater than human-health benchmarks in untreated source water. Naturally occurring contaminants are mostly derived from the natural geologic materials that make up the aquifers from which wellwater is withdrawn. Man-made contaminants were also found in untreated water sampled from the public wells, including herbicides, insecticides, solvents, disinfection by-products, nitrate, and gasoline chemicals. Man-made contaminants accounted for about one-quarter of contaminant concentrations greater than human-health benchmarks, but were detected in 64 percent of the samples, predominantly in samples from unconfined aquifers. Source: http://beforeitsnews.com/news/47/629/Well_Water_Contamination_A_Health_Risk_for_More_Than_One_Third_of_U.S.Population_Say_USGS_Scientists.html

## North Dakota Homeland Security Contacts

**To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(In ND only)**; Email: ndslic@nd.gov ; Fax: **701-328-8175**
**State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455**
**US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241**

**To contribute to this summary or if you have questions or comments, please contact:**

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**


NDDES
Homeland Security
State Radio
NORTH DAKOTA
STATE PATROL
NORTH DAKOTA
STRENGTH FROM THE SOIL
NATIONAL GUARD